Princeton

ユーザーズマニュアル

安全上のご注意

ご使用の前にこの「安全上のご注意」をよくお読みの上、正しくお使いください。

お読みになった後は、いつでも見られるところに大切に保管してください。

警告	この表示を無視して、誤った取り扱いをすると、人が死亡または重傷を負う可能性が想定される内容を示しています。
注意	この表示を無視して、誤った取り扱いをすると、人が傷害を負う可能性が想定される内容または物的損害の発生が想定される内容を示しています。

△ 記号は注意(警告を含む)を促す内容があることを告げるものです。
○ 記号は禁止の行為であることを告げるものです。
■ 記号は行為を規制したり指示する内容を告げるものです。

警　告	
	万一、次のような異常が発生したときは、そのまま使用しないでください。 ・煙が出ている、変な匂いがするなど異常のとき。 ・内部に水や金属物が入ってしまったとき。 ・落としたり、キャビネットが破損したとき。 このような異常が発生したまま使用していると、火災や感電の原因となります。煙りが出なくなるのを確認してから販売店に修理を依頼してください。お客様による修理は危険ですから絶対におやめください。
	この製品を分解・改造しないでください。火災や感電の原因となります。
	この製品を水などの液体で濡らさないでください。感電や故障の原因となります。

注　意	
	直射日光やストーブのような熱器具の近くなど、高温になるところに放置すると、変形・変質をまねくため、ご注意ください。
	次のような場所には置かないでください。火災・感電・けがの原因となることがあります。 ・湿気やほこりが多い場所 ・ぐらついた台の上や傾いた所などの不安定な場所 ・調理台や加湿器のそばなどの油煙や湯気があたる場所
	汚れがひどい場合は、中性洗剤等で拭き取ってください。シンナーやベンジンなどは、絶対に使わないでください。

御利用上のご注意

・本製品は高精度な半導体センサーと指紋解析アルゴリズムにより、登録された指紋データを元に認証を行っておりますが、非常に類似した第三者の指紋、登録された指紋の状態、設定された認識率、ノイズ、センサーの汚れ、センサーの読み取り誤差など、様々な要因のために登録されていない指紋による認証を回避できるとは限りません。

ごくまれに、指紋を登録・認証できない場合があります。指紋を認証できなかったことによって発生する動作障害、データの損失、あるいは他の偶発的または必然的な損害に対しては、弊社では一切の責任を負いかねますので、御了承ください。

指紋を認証できなかったことによって発生する動作障害、データの損失、あるいは他の偶発的または必然的な損害に対しては、弊社では一切の責任を負いかねますので、御了承ください。

弊社では、本装置の運用を理由とする損失、逸失利益等の請求につきましてはいかなる責任も負いかねますので、あらかじめご了承ください。

・本製品の御利用によるコンピュータ本体や他の機器の不具合、特定のハードウェア、ソフトウェア、周辺機器に対する適性、またインストールされたソフトウェア相互の適性などに起因する動作障害、データの損失、あるいは他の偶発的または必然的な損害に対しては弊社では一切の責任を負いかねますので、御了承ください。

購入された当社製品は、一般 OA 機器として使用されることを目的に開発・製造されたものです。当社製品を航空機・列車・船舶・自動車などの運行に直接関わる装置・防災防犯装置・各種安全装置など機能・精度において高い信頼性・安全性が必要とされる用途に使用される場合は、これらのシステム全体の信頼性および安全維持のためにフェールセーフ設定や冗長設計の措置を講じるなど、システム全体の安全設計にご配慮いただいた上で当社製品をご使用ください。

本装置は、医療機器、原子力設備や機器、航空宇宙機器、輸送設備や機器など、人命に関わる設備や機器、および高度な信頼性を必要とする設備や機器などへの組み込みや制御等の使用は意図されておりません。これら設備や機器、制御システムなどに本装置を使用され、人身事故、財産損害などが生じても、弊社はいかなる責任も負いかねます。

・当社製品は、航空宇宙機器、幹線通信機器、原子力制御機器、生命維持に関わる医療機器、24 時間稼働システムなど、極めて高い信頼性・安全性が必要とされる用途への使用を意図しておりませんので、これらの用途にはご使用にならないでください。

本書の内容に関しては将来予告なしに変更されることがあります。

本機に添付の CD-ROM、フロッピーディスクは、本機のみでご使用ください。

ソフトウェアの全部または一部を著作権の許可なく複製したり、複製物を頒布することは禁じられております。

本書の内容については万全を期して作成いたしましたが、万一ご不審な点や誤り、記載もれなどお気付きのことがありましたら、ご購入元、またはお問い合わせ窓口へご連絡ください。落丁、乱丁本はお取り替えいたします。

目次

U-CLEF/F とは

U-CLEF/F は、Windows98 SE/Me/2000/XP のログオン、スクリーンセーバー、ファイルの暗号化など、コンピュータのセキュリティを高めるさまざまな機能を搭載しています。U-CLEF/F の導入およびインストール手順などをこのマニュアルに詳しく説明しますので、導入する前に必ずこのマニュアルをお読み下さい。

U-CLEF/F とは

この度は弊社の指紋認証システム製品「U-CLEF/F」をお買い上げ頂き、誠にありがとうございます。

「U-CLEF/F」は、「指紋」をキーとして使用し、最新の富士通製指紋センサーと独自のセキュリティソフトウェアを組み合わせることにより、コンピュータのセキュリティを高める機能を提供する製品です。この U-CLEF/F を利用することによって、個人データやコンピュータの使用を保護することができるようになるため、これまでのパスワードだけによるセキュリティよりも優れたセキュリティソリューションを提供します。

U-CLEF/F の利用方法やセットアップは簡単です。ユーザーは自らの指紋を使ってシステムに登録することにより、登録ユーザーだけがコンピュータやデータを利用することができるようになります

➔ 「U-CLEF/F」で実現する機能

- 指紋を利用した Windows ログオン
- 暗号化されたファイルを開くときに指紋認証が必要な専用のファイル暗号化機能
- 解除時に指紋認証が必要なスクリーンセーバー機能
- 解除時に指紋認証が必要なコンピュータをロック機能
- 登録されたユーザーごとに、1 日の利用時間の制限を設定

これらの機能は、「U-CLEF/F」本製品（指紋センサーとバイオガードソフトウェア）によって実現されます。

ご注意：

ハードディスクの故障、ウイルス若しくはその他の問題により生じたファイル及びデータベースの破損、紛失などによりソフトウェアが正常に動作しない場合があります。このような自体を避ける為に定期的なバックアップ併用してご使用することをお薦めいたします。

U-CLEF/F 機能一覧表

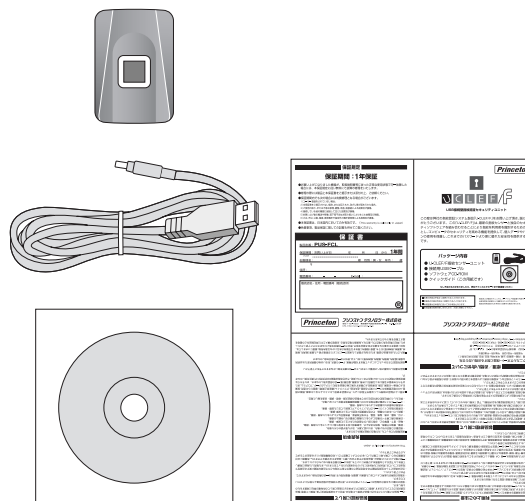
	説 明
ユーザーの登録	権限には下記の 2 つがあります: 1. **ユーザー**: 自分のデータが変更でき、また所属グループにユーザーカウントが追加できます。 他のユーザーの情報は見たり修正することはできません。 2. **管理者**: ユーザーの追加登録、削除、参照及び全てユーザーの権限が変更できます。ユーザーは 1 人あたり2つの指紋を設定/登録します。設定するパスワードは、最大 15 文字が入力可能です。 最大 100 ユーザーのアカウントが登録管理可能です。 ユーザーは自分のパスワードと指紋データしか変更できません。他人のデータを変更する権限がありません。
Window ログオン	システムにログオンする際、あらかじめ登録された指紋によって適切なユーザーとして自動的にログオンします。登録されていない指紋の場合は、指紋入力画面が表示され、ログオンすることはできません。
スクリーンセーバー	スクリーンセーバーを利用した際、復帰するときに指紋認証を必要とします。登録された正しいユーザーの指紋でない限り、元の画面に戻ることができません。 一時的にコンピュータを利用していないときに、第三者に不正アクセスさせないようにします。 ホットキーを経由してすぐスクリーンセーバーを起動することもできます。
ファイルの暗号化	登録されている指紋をデータキーとして、指定したファイルを暗号化して、第三者がファイルを開くことができないようにすることができます。複数のファイルが同時に暗号化可能です。フォルダーが暗号される場合、その中のすべてファイルが暗号されます（まとめてひとつのファイルにすることはできません）。 暗号されたファイルの復号はあらかじめ定義された指紋をもつユーザーのみです。また該当ユーザーのグループ内のアカウントも復号することができます。それ以外のグループ以外のユーザー（管理者も含む）は復号する権限がありません。
グループ機能	管理者は U-CLEF/F を利用して指紋アカウントを持つユーザーを、他のコンピュータ（ユーザー）同士でグループとして所属させることができます。これにより同一グループに属しているユーザーどうしで、暗号化したファイルを開いたり修正したりすることができます。
使用時間の制限	ユーザーごとに、1 日あたりの最大利用時間を設定できます。設定した時間を経過すると、そのユーザーはコンピュータを利用できずに、自動的にシャットダウンします。
その他	ログファイルに最大 30,000 個のアクセス記録が保存できます。この情報には、ユーザーが行ったログオン、新規登録、削除、暗号・復号などの動作情報が記録されます。

U-CLEF/F を使うためには

それではここから、実際に U-CLEF/F をコンピュータにセットアップする方法を紹介していきましょう。

U-CLEF/F を動作させるために必要な条件

➔ パッケージ内容

1. バイオガード本体（指紋センサーユニット）
2. USB ケーブル
3. ソフトウェアCD-ROM
4. クイックインストレーションガイド

ご注意：

もし不足しているものがありましたら、弊社テクニカルサポートまで御連絡ください。

➔ 動作システム条件

ハードウェア

CPU:	Pentium PC 以上
メモリ：	６４MB以上
ハードディスク：	8MB 以上空き容量があること
ビデオカード：	SVGA（800×600 ピクセル）以上の表示をサポートしていること
インターフェイス：	USB1.1 ポートを標準装備していること
ドライブ：	CD－ROMドライブを利用可能であること

対応 OS

U-CLEF/F が動作する OS は下記のものです

Windows 98SE

Windows Me

Windows ２０００

Windows XP

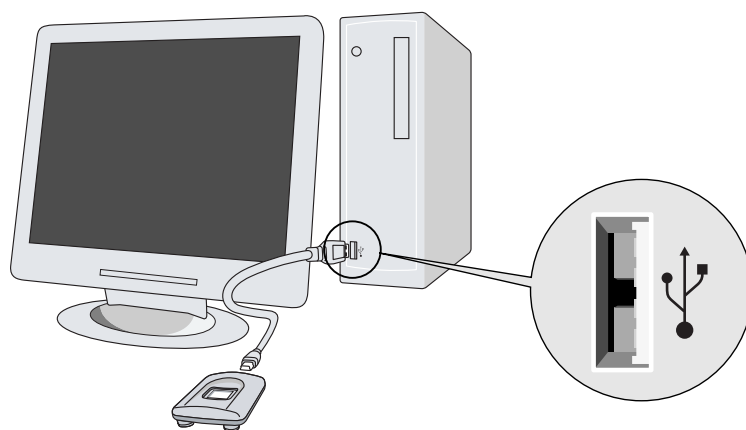
ご注意：

：Windows 98、Windows NT 4.0、Windows 95、Windows 2003、Mac OS、Unix、Linux には対応しておりません

U-CLEF/F のセットアップ

U-CLEF/F はハードウェア（指紋センサー）とソフトウェア（バイオガードセンター）を組み合わせて利用します。ハードウェアをコンピュータにつないで利用するには、あらかじめ専用のドライバソフトをシステムにインストールする必要があります。

➔ U-CLEF/F をコンピュータに接続する

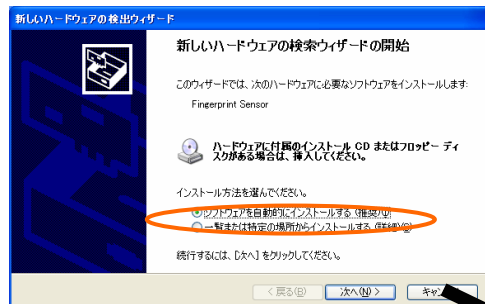
U-CLEF/F は、コンピュータに用意されている「USB」ポートと呼ばれるインターフェイスに接続して利用します。お使いになられているコンピュータのどこに USB ポートがあるのかは、マニュアルを参照してください（USB ポートは、下図にあるマークが付いています）。

ご注意：

USB ハブを利用して U-CLEF/F を接続した場合の動作保証はいたしません。コンピュータ本体に設けられている USB ポートに直接接続して利用してください。USB 拡張ボードを利用した場合の動作保証はいたしません。付属の USB ケーブル以外のものを使った場合の動作保証はいたしません。

ドライバーのインストール

U-CLEF/F のセンサーユニットをコンピュータに接続すると、新しいハードウェアを見つけたことを知らせるメッセージが表示されますので、次の手順に従って、ドライバーソフトのインストールを行います。

➔ Windows XP の場合

1:コンピュータの電源を入れ、Windows を起動し、指紋センサーにつながっている USB ケーブルをコンピュータ本体の USB コネクターへ接続します。

2:新しいハードウェアを見つけたことを知らせるメッセージが表示されますので、「一覧または特定の場所からインストールする(詳細)」を選択し、「次へ」ボタンをクリックします。

3:添付されている CD-ROM、パソコンの CD-ROM ドライブにを挿入してください。「次の場所で最適のドライバを検索する」を選択、そして「次の場所を含める」チェックボックスを選択して、右の「参照」ボタンをクリックします。 そして¥Driver のディレクトリを選択してから、「次へ」ボタンをクリックします。

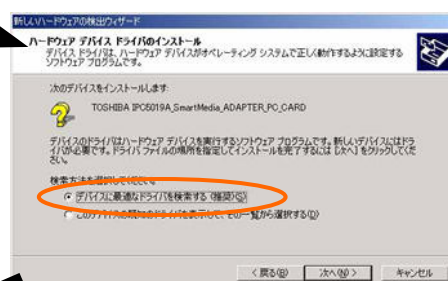
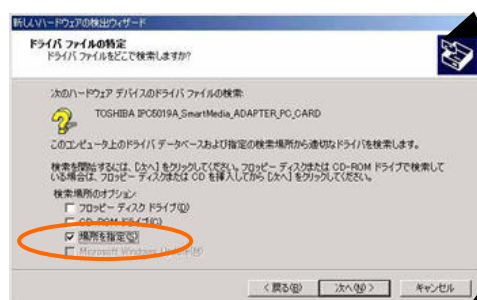
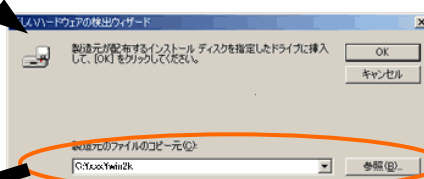
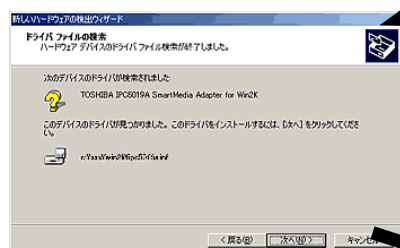
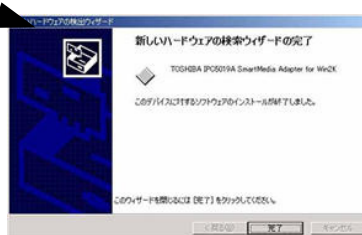
4:インストール中に、「このハードウェア TACOMA MBF2000 Module を使用するためにインストールしようとしているソフトウェアは、Windows XP との互換性を検証する Windows ロゴテストに合格していません」というメッセージが表示される場合があります。そのときは「続行」ボタンを押してインストールを継続してください。

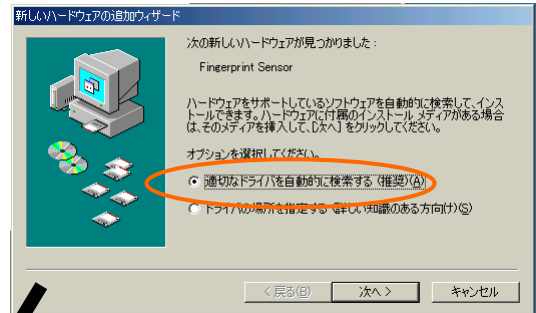
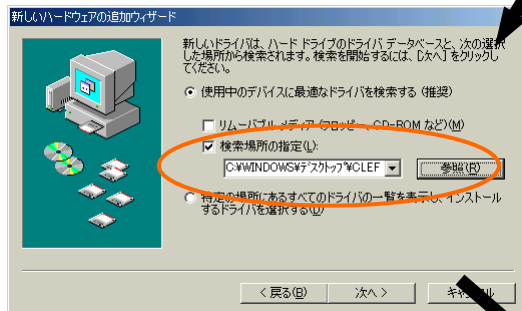
5:ドライバのインストール作業が継続して行なわれ、「新しいハードウェアの検索ウイザードの完了」が表示されたら正常にインストールは終わりです。「完了」ボタンをクリックしてください。

➔ Windows 2000 の場合

1:コンピュータの電源を入れ、Windows を起動し、指紋センサーにつながっている USB ケーブルをコンピュータ本体の USB コネクターへ接続します。新しいハードウェアを見つけたことを知らせるメッセージが表示され、ドライバのインストールが開始されます。

2:「新しいハードウェアの検索ウイザード」という画面が表示されますので「次へ」を押して先に進めてください。

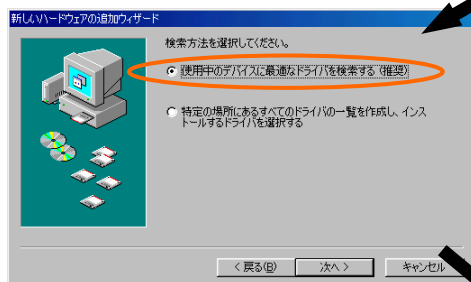
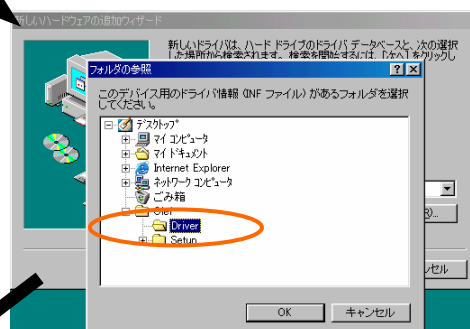
3:「次のデバイスをインストールします」とメッセージが表示されるので、「デバイスに最適なドライバを検索する」をチェックして「次へ」を押してください。

4:「場所を指定」にチェックをいれて、「次へ」を押してください。

5:添付されている CD-ROM、パソコンの CD-ROM ドライブにを挿入してください。その後「参照」ボタンを押して、CD-ROM ドライブ内の「Driver」フォルダを指定したあと、OK ボタンを押してください。

6:適切なドライバが自動的に検索されて画面に表示されますので、そのまま「次へ」ボタンを押してください。

7:ドライバのインストール作業が継続して行われ、「新しいハードウェアの検索ウイザードザの完了」が表示されたら正常にインストールが終わりました。「完了」ボタンをクリックしてください。

➔ Windows Me の場合

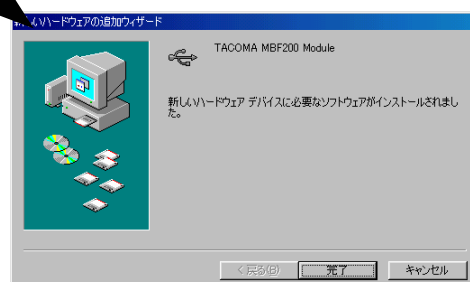
1：コンピュータの電源を入れ、Windows を起動し、指紋センサーにつながっている USB ケーブルをコンピュータ本体の USB コネクターへ接続します。「一覧または特定の場所からインストールする(詳細)」を選択し、「次へ」ボタンをクリックします。

2：「使用中のデバイスに最適なドライバを検索する」という画面が表示されますので、添付されている CD-ROM、パソコンの CD-ROM ドライブに挿入してください。「次の場所で最適のドライバを検索する」を選択、そして「次の場所を含める」チェックボックスを選択して、右の「参照」ボタンをクリックします。 そして¥Driver のディレクトリを選択してから、「次へ」ボタンをクリックします。

3：「TACOMA MBF2000 Module」ドライバが自動的に検索されて画面に表示されますので、そのまま「次へ」ボタンを押してください。

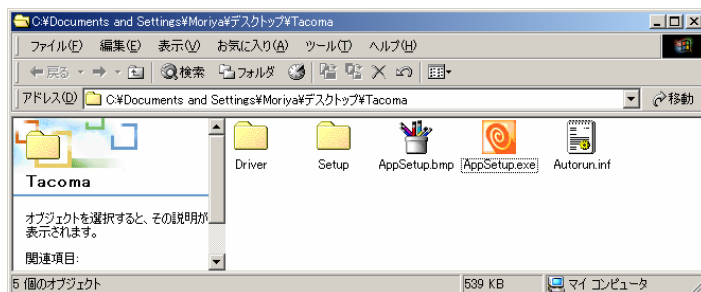
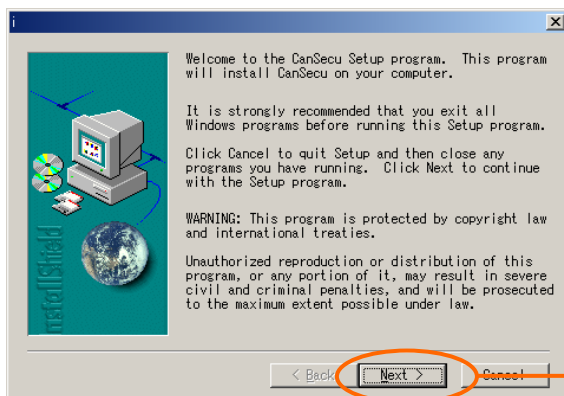
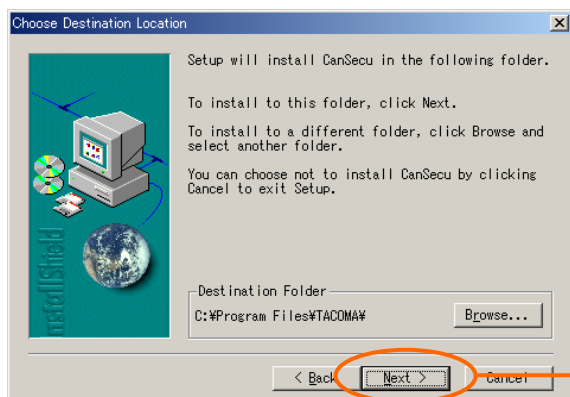
4：システムは「TACOMA MBF2000 Module」と認識し、必要なドライバが自動的にインストールされます。

➔ Windows 98 SE の場合

1:コンピュータの電源を入れ、Windows を起動し、指紋センサーにつながっている USB ケーブルをコンピュータ本体の USB コネクターへ接続しますので、「次へ」ボタンをクリックします。

2:画面に「使用中のデバイスに最適なドライバを検索する」にチェックをいれ、「次へ」ボタンを押します。

3:ドライバのある場所を尋ねてくるので、添付されている CD-ROM、パソコンの CD-ROM ドライブにを挿入してください。その後「参照」ボタンを押して、CD-ROM ドライブ内の「Driver」フォルダーを指定したあと、OK ボタンを押してください。

4:「TACOMA MBF2000 Module」ドライバが自動的に検索されて画面に表示されますので、そのまま「次へ」ボタンを押してください。

5:システムは「TACOMA MBF2000 Module」と認識し、必要なドライバが自動的にインストールされます。

バイオガードセンターのインストール

1. U-CLEF/F のパッケージに付属している CD-ROM をコンピュータの CD-ROM ドライブ（もしくは DVD-ROM ドライブ）に入れ、「AppleSetup.exe」をクリックします。 もしインストール画面が自動的に表示されない場合、Windows 画面のスタート→ファイル名を指定して実行→“D:¥AppSetup¥SETUP.EXE”を入力して、「OK」ボタンをクリックして下さい。

2. インストール画面が表示されますので、画面に表示されるメッセージに従って、インストールを進行します。

「Next」ボタンを押して、インストールを継続すると、アプリケーションの保管先を指定して、「Next」ボタンを押して、インストールを継続すると、システムにアプリケーションのインストールが開始されます。

その後、U-CLEF/F の管理者に関するアカウントや指紋情報を登録する画面が表示されます。下図の注意メッセージが表示されたら、OK ボタンを押してください。

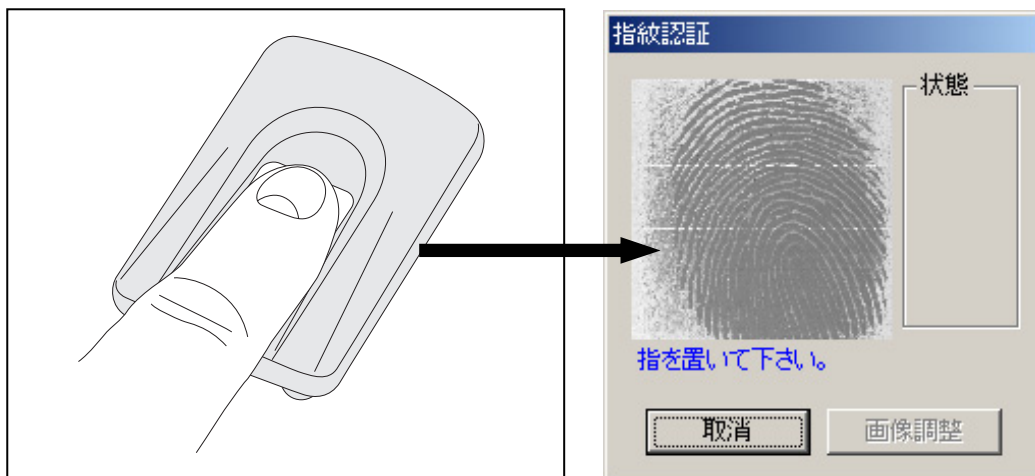
ボタンを押すと「データ設定」というウィンドウが表示されますので、まず名前の欄に、管理者（U-CLEF/F をインストールしたコンピュータをメインに利用するユーザー）のアカウントとパスワードを入力してください。

3. 管理者の名前（ユーザー名）とパスワードを入力してください。

ご注意：

名前とパスワードを入力するとき、Windows システムと一致しないと、ネットワークにアクセスできない恐れがあります。必ず両方の名前とパスワードを同じ設定にして下さい。

4. 登録したい指を「指 1」のなかから選ぶと、指紋を取り込む画面が表示されます。

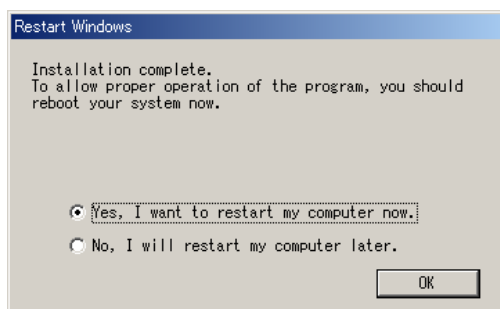
5. 指紋センサーに、登録したい指を乗せますと、「指紋認証」画面に指紋のパターンが表示され、バイオガードセンターに登録されます。登録が終わると、データ設定の画面に戻ります。

指をセンサーに乗せると、画面にはセンサーが読み取った指紋パターンが表示されます

指を乗せると、画面にはセンサーが読み取った指紋パターンが表示されます

ご注意：

センサーに正しい方向で指を乗せてください強く押し付けたり、軽く乗せていたりすると、センサーは正しく指紋を読み取ることができません。どのような強さで指を乗せて登録したのかを忘れないようにしてください。

6. 次に、別の指を使って、異なる指紋を登録します。これは、何らかの問題で（指を怪我した場合など）でも認証できるように、予備の指紋情報を登録するためです。ウィンドウ右側の「指2」の欄から登録したい指を選択して、「指　1」と同様に指紋を登録します（これは必須ではありません）

7. 2 つの指紋が登録できたら、「確認」ボタンを押すと、システムの再起動を促すメッセージが表示されます。「Yes, I want….」をチェックして「OK」ボタンを押して、システムを再起動して下さい（No,I will…を選んで OK ボタンを押した場合、システムは再起動しません。ただし再起動するまで、指紋認証機能は利用できません）。

再起動後、U-CLEF/F による指紋認証が利用できるようになります。再起動してシステムにログオンするときには、「指紋認証」の画面が表示されますので、先ほど登録した指を乗せて、コンピュータにログオンしてください。

バイオガードセンターを利用する

バイオガードセンターは、指紋センサーで認識された指紋情報を基に、コンピュータへのログオンに関する設定やスクリーンセーバーやPCロック機能、指紋をキーとしたファイルの暗号化などを設定するソフトウェアです。

U-CLEF/Fを活用するには、このバイオガードセンターで設定を行う必要があります。ここではバイオガードセンターの利用法について解説します。

U-CLEF/F の認証機能とは

「認証」とは指紋やパスワードを通して合法的にユーザーを判定することを言います。「バイオガードセンター」、「ファイルの暗号化、復号化」、「スクリーンセーバー」あるいは「アンインストール」等の機能を実行するとき、システムはユーザーに認証することを要求します。認証が正しくないと、次のステップには進めません。

指紋センサーをコンピュータに接続すれば、指紋認証が実行できます。

指紋センサーをコンピュータに接続しない場合、代わりにパスワードで認証します。ユーザーの名前とパスワードを入力して、「確認」ボタンをクリックしてシステムを起動します。

Windows ログオン

バイオガードソフトウェアは指紋認証機能により、従来のパスワード認証でのログオンが不要になりました。ユーザーは登録した指紋で照合認証すればシステムへ簡単にログオンすることができます。

指をセンサーに乗せると、画面にはセンサーが読み取った指紋パターンが表示されます

指を乗せると、画面にはセンサーが読み取った指紋パターンが表示されます

Windows にログオンする際は OS 環境によって異なる場合があります。Windows2000/XP を使用する場合、コンピュータがドメインに属すると、ユーザーはドメインあるいはローカルコンピュータかを選択して登録することができます。(指紋入力画面の下に下方向矢印のボタンをクリックして選択できます)

指紋認証確認後、ユーザーは Windows システムにログオンできます。指紋センサーをコンピュータに接続していない場合、パスワード入力でシステムにログオンして下さい。

なお、システムに登録するとき、登録画面をそのままにしておくと、指紋センサーが省電力のためログオンできなくなります。このとき指紋入力画面に表示されている「再試行」ボタンを押すことにより、引続き指紋登録を行うことができます。

ご注意:

「バイオガードセンター」のパスワードは必ず Windows およびネットワークログオン時に使用しているものと同一にしてください。ユーザーは Windows パスワードを変更することができます。"コントロールパネル→パスワード→パスワードの変更"にパスワードを変更後、"バイオガードセンター"のパスワードも同時に変更されます。

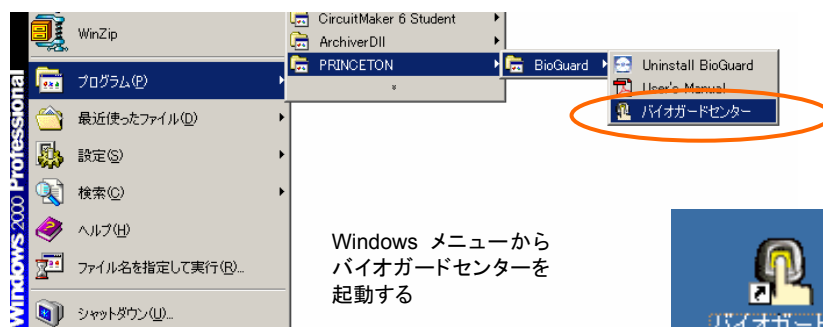
バイオガードセンターの機能

U-CLEF/F でログオン機能など、コンピュータでのセキュリティ機能を司るソフトウェアが、「バイオガードセンター」です。このソフトを使って、指紋登録やユーザーの管理、システム設定などを行います。「バイオガード」に用意されている機能は下表のとおりです。

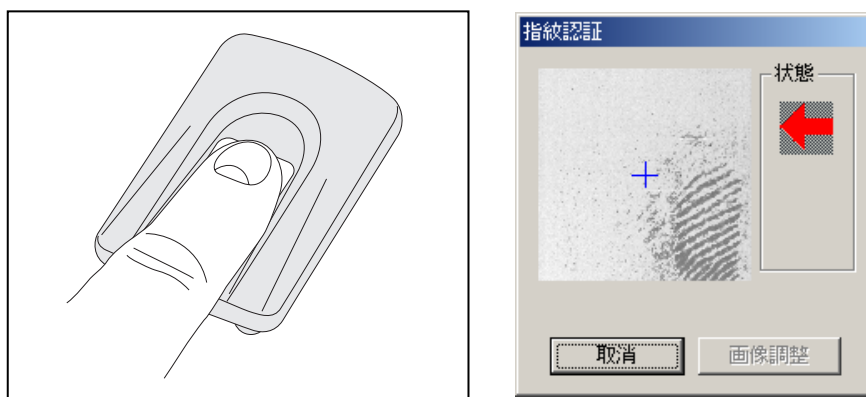
➔ バイオガードで利用できる機能

	説　明
ユーザーの登録	権限には下記の 2 つがあります: 1. **ユーザー**: 自分のデータが変更でき、また所属グループにユーザーカウントが追加できます。 他のユーザーの情報は見たり修正することはできません。 2. **管理者**: ユーザーの追加登録、削除、参照及び全てユーザーの権限が変更できます。ユーザーは 1 人あたり2つの指紋を設定/登録します。設定するパスワードは、最大 15 文字が入力可能です。 最大 100 ユーザーのアカウントが登録管理可能です。 ユーザーは自分のパスワードと指紋データしか変更できません。他人のデータを変更する権限がありません。
Window ログオン	システムにログオンする際、あらかじめ登録された指紋によって適切なユーザーとして自動的にログオンします。登録されていない指紋の場合は、指紋入力画面が表示され、ログオンすることはできません。
スクリーンセーバー	スクリーンセーバーを利用した際、再復帰するときに指紋認証を必要とします。登録された正しいユーザーの指紋でない限り、元の画面に戻ることができません。 一時的にコンピュータを利用していないときに、第三者に不正アクセスさせないようにします。 ホットキーを経由してすぐスクリーンセーバーを起動することもできます。
ファイルの暗号化	登録されている指紋をデータキーとして、指定したファイルを暗号化して、第三者がファイルを開くことができないようにすることができます。複数のファイルが同時に暗号化可能です。フォルダーが暗号される場合、その中のすべてファイルが暗号されます（まとめてひとつのファイルにすることはできません）。 暗号されたファイルの復号はあらかじめ定義された指紋をもつユーザーのみです。また該当ユーザーのグループ内のアカウントも復号することができます。それ以外のグループ以外のユーザー（管理者も含む）は復号する権限がありません。
グループ機能	管理者は U-CLEF/F を利用して指紋アカウントを持つユーザーを、他のコンピュータ（ユーザー）同士でグループとして所属させることができます。同一グループに属しているユーザーどうしで、暗号化したファイルを開いたり修正したりすることができます。
使用時間の制限	ユーザーごとに、1 日あたりの最大利用時間を設定できます。設定した時間を経過すると、そのユーザーはコンピュータを利用できずに、自動的にシャットダウンします。
その他	ログファイルに最大 30,000 個のアクセス記録が保存できます。この情報には、ユーザーが行ったログオン、新規登録、削除、暗号・復号などの動作情報が記録されます。

バイオガードセンターの起動

スタート→プログラム→Princeton→BioGUard からバイオガードセンターを選んで起動するか、またはデスクトップ上のショートカットアイコンをダブルクリックする、もしくはタスクバーにあるアイコンをダブルクリックします。

デスクトップに作成されたバイオガードセンターのショートカットアイコン

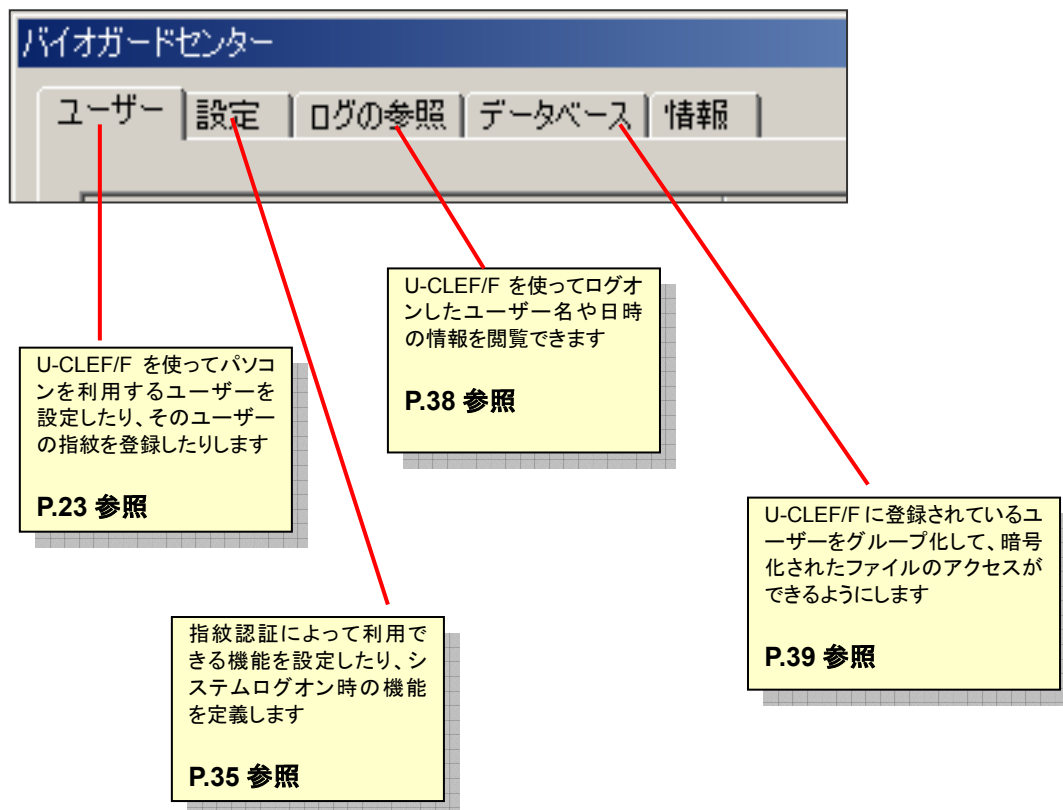
タクスバーに作成されたバイオガードセンターのショートカットアイコン

すると最初に管理者の指紋を入力する画面が表示されますので、登録した指を指紋センサーに置きます。

認識した指紋が、バイオガードセンターに登録されているものであれば、バイオガードセンターが起動します。正常に起動すると、登録されているユーザーを一覧表示する画面が表示されます。もし乗せた指の位置がセンサーからずれている場合には「状態」の欄に矢印が表示されますので、その方向に指を移動させてください。

ご注意:

もし認識された指紋が、バイオガードセンターにて「ユーザー」権限で登録されたものであった場合、そのユーザー以外の情報は表示されません。

➔ バイオガードセンターの機能の切り替え

バイオガードセンターでは、画面に表示されているウィンドウの上にあるタブを選択することによって、用意されている機能を切り替えることができます

➔ ユーザー機能

U-CLEF/F を利用してコンピュータにログオンするユーザーに関する情報を登録／参照します。

認識した指紋が、バイオガードセンターに登録されているものであれば、バイオガードセンターが起動し、登録されているユーザーを一覧表示する画面が表示されます。この画面で利用できる機能は下図のとおりです。

ユーザーの登録

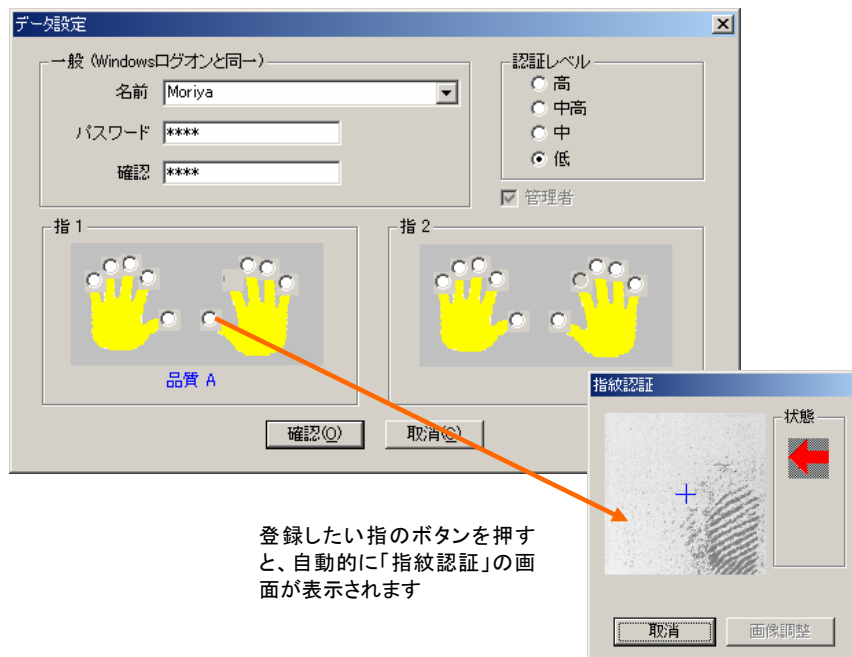
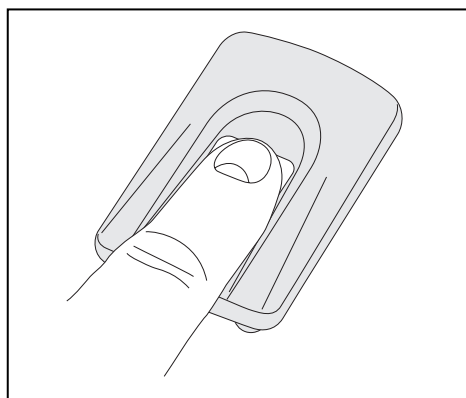
U-CLEF/F を利用するユーザーを新しく追加します。追加する手順は、まず「ユーザー」画面の下にある「新規登録」のボタンを押すと、「データ設定」というウィンドウが表示されます。ここで設定できる機能は下図のとおりです。

新規にユーザーを登録するには、ユーザー名の欄にユーザー名とパスワードを入力したあと、指紋を登録します。名前（ユーザー名）とパスワードを入力してください。そして登録したいユーザーの権限を「ユーザー」「管理者」どちらかを選択してください。

ご注意：

名前とパスワードを入力するとき、Windows システムに登録されたものと一致しないと、ネットワークにアクセスできない恐れがあります。必ず両方の名前とパスワードは、Windows システムに登録されたものと同じ設定にして下さい。

登録したい指を「指 1」のなかから選ぶと、指紋を取り込む画面が表示されます。

登録したい指のボタンを押すと、自動的に「指紋認証」の画面が表示されます

指紋センサーに、登録したい指を乗せます。

指をセンサーに乗せると、画面にはセンサーが読み取った指紋パターンが表示されます

指を乗せると、画面にはセンサーが読み取った指紋パターンが表示されます

ご注意：

センサーに正しい方向で指を乗せてください強く押し付けたり、軽く乗せていたりすると、センサーは正しく指紋を読み取ることができません。最初に登録したときに指をどのように乗せたのかを忘れないようにしてください。

「指紋認証」画面に指紋のパターンが表示され、バイオガードセンターに登録されます。登録が終わると、データ設定の画面に戻ります。

これでユーザーの登録は完了です

次に、別の指を使って、異なる指紋を登録します。これは、何らかの問題で（指を怪我した場合など）でも認証できるように、予備の指紋情報を登録するためです。ウィンドウ右側の「指 2 欄から登録したい指を選択して、「指 1」と同様に指紋を登録します（これは必須ではありません）

指紋の登録が終われば「確認」ボタンを押してバイオセンターの「ユーザー」画面に戻り、いま登録したユーザーが表示されていることを確認してください。

ユーザープロファイル

U-CLEF/F に登録されているユーザーの権限は、下記のとおりに表示されます。

 管理者：この管理者はユーザーの追加登録、削除、参照及び全てユーザーの権限が変更できます。

 利用者：現在ログオンしていない非使用中の管理者です。上記の管理者と同じくユーザーの追加登録、削除、参照及び全てユーザーの権限が変更できます。

 ユーザー：このユーザーは、自分のパスワードと指紋データしか変更できません。

ユーザー情報の変更

登録されているユーザーの情報を変更します。

登録データ(指紋及びパスワード)は、ログオンしているユーザー自身の情報しか変更することができません。ログオンしているユーザーが、自分の情報（登録している指紋情報やパスワード、権限など）を変更できます。

指紋データを変更する場合

指のボタンを押して「変更」ボタンをクリックして、登録した指の変更ができます。

パスワードを変更する場合

パスワードのボックスに、新しいパスワードを入力して「確認」ボタンを押してください。

権限を変更する：登録したユーザーは管理者であれば、この管理者は、自身や他のユーザーの設定を変更できます。但し、他の管理者の設定を変更するができません。

異なるユーザーの情報で変更できる内容

- 利用時間の制限
- 権限の変更（ユーザーから管理者）

この 2 点になります。

ユーザーの削除

管理者権限を持つ場合、自分のユーザーデータと、権限が「ユーザー」になっている他のユーザーのデータは削除することができますが、他の管理者のデータを削除することはできません。

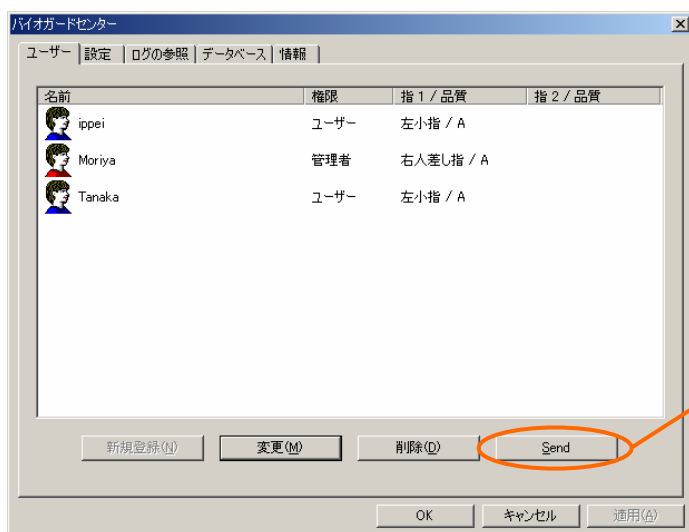
登録したユーザーを削除すると、そのユーザーに関するデータを回復させることはできません。もし、そのユーザーが作成した暗号化ファイルがある場合、そのファイルは回復させることはできなくなりますので、ご注意ください。

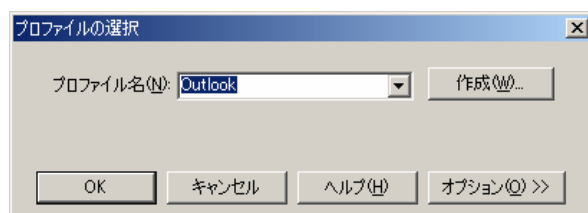
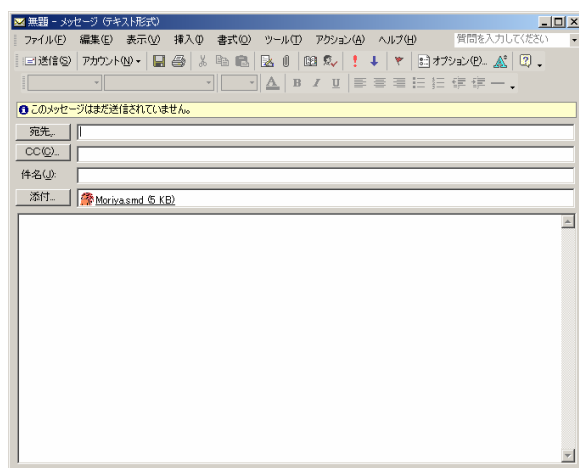
削除する前に特に暗号化ファイルが残っていないかどうかを確認して下さい。

➔ Send 機能

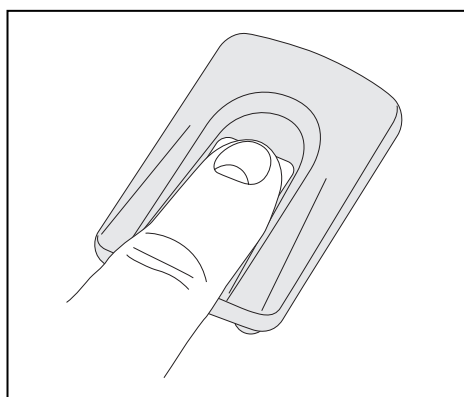
いま利用しているコンピュータで登録した指紋のテンプレートをファイルとして作成し、電子メールで他人に送ることによって他のコンピュータで暗号化されたファイルを開くことができるようにするための機能です。この send 機能を利用することによって、重要なデータを電子メールなどで送ることが可能となります。

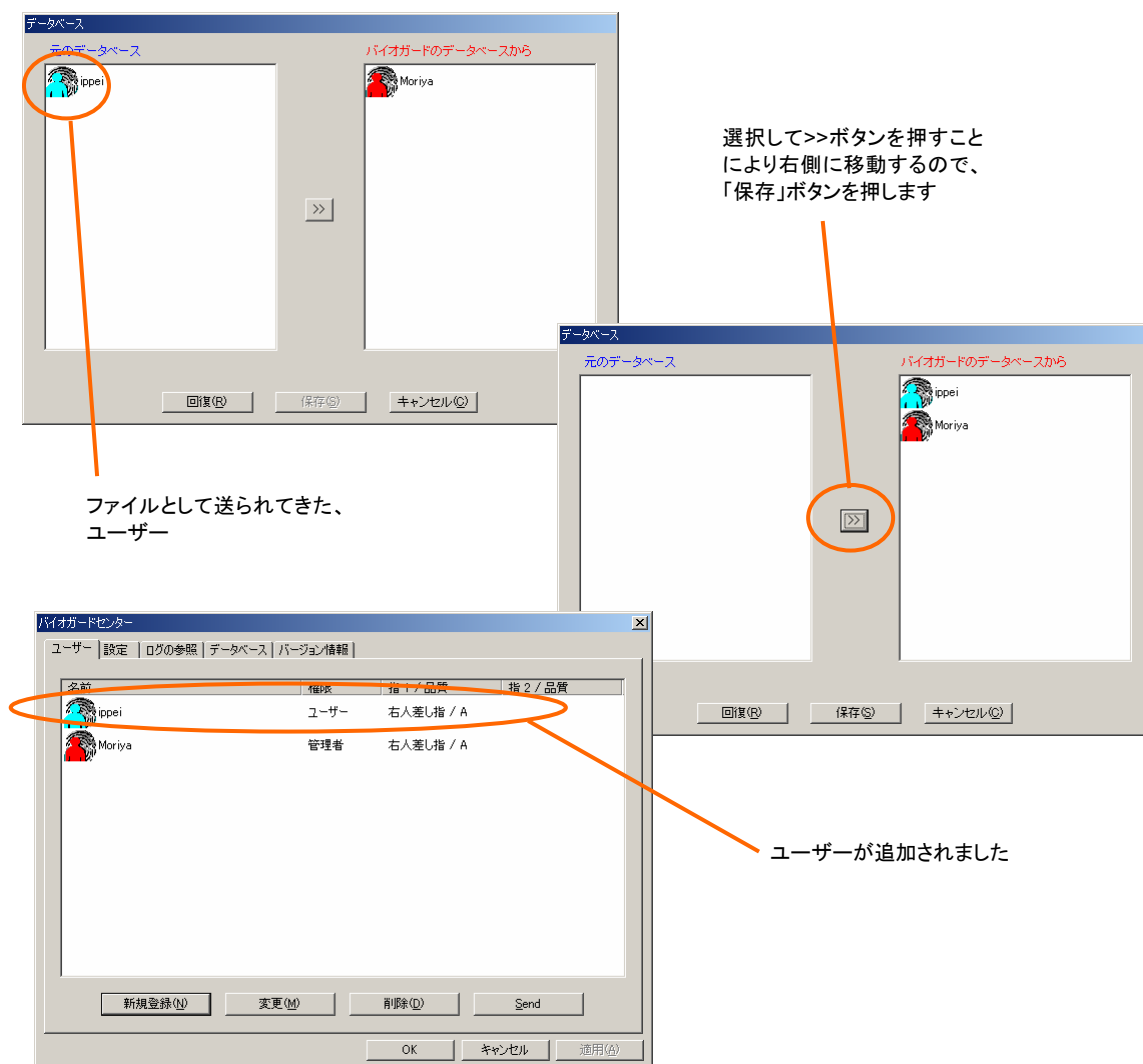
➔ ファイルの送信

バイオガードセンターの画面でユーザーを選択し、「send」ボタンを押します。

次に、同時にグループとして指紋のテンプレートファイル内に所属させたいユーザーを追加する画面が表示されますので、追加したいユーザーがいる場合は「>>」ボタンを押してグループメンバーに追加させてください。作業が終わったら、「OK」ボタンを押してください。

利用するメーラーを選択する画面が表示されますので、アプリケーションを選択し、「OK」ボタンを押してください。もし登録されていない場合は、右側の「作成」ボタンを押してプロファイルを新しく登録してください。

OKボタンを押すとメーラーの新規メール画面が作成され、添付ファイルに指紋認証用テンプレートファイル（拡張子が.smdとなっているファイル）が添付されます。送信先のメールアドレスや本文を記入したあと、メールを送信してください。

➔ 受信側

メールを受け取った側は、添付された指紋認証用テンプレートファイルをダブルクリックするか、デスクトップにコピーしたあとにファイルを開いてください。

すると指紋認証画面が表示されますので、そのコンピュータに登録されているユーザーの指紋を認識させます。

続いて、グループに追加する画面が表示されますので、送られてきた指紋認証ユーザーの情報を確認したうえ、

追加したいユーザーを選んで「保存」ボタンを押します。

別のコンピュータで定義されたユーザーを自分のコンピュータ側に登録することにより、ユーザーが作成した暗号化されたファイルも自分で開くことができるようになります。

指紋登録のヒント

指を指紋センサーに軽く水平に置きます。

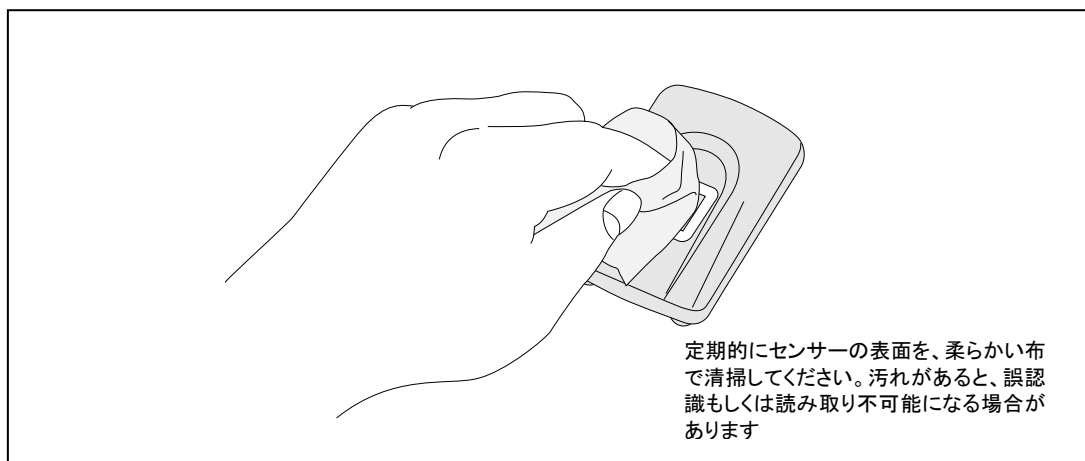
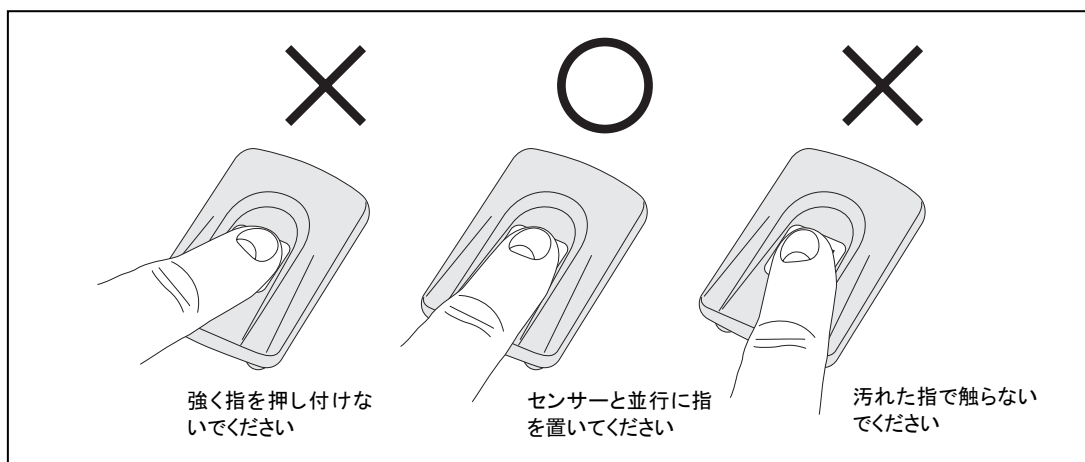
指紋画像がデバイスにキャプチャーされてから、一旦指をデバイスから離して、2〜3 秒後再度デバイスに置きます。

指を置くときはセンサーに強く押し付けないでください

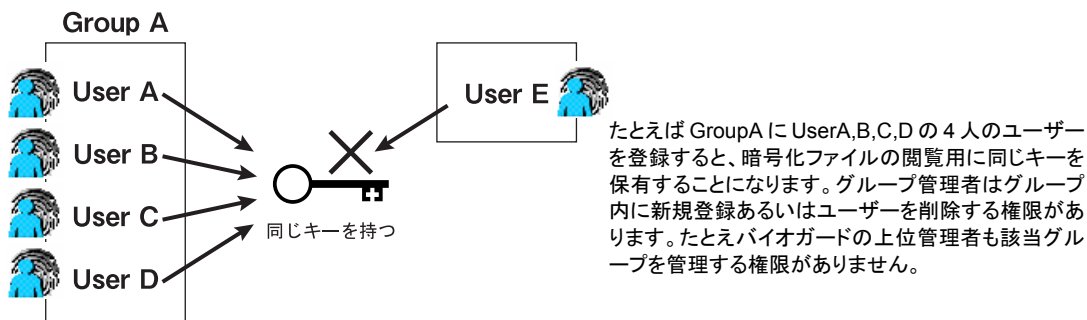
指が乾燥している場合、指を少し湿らせた布で拭いてください。

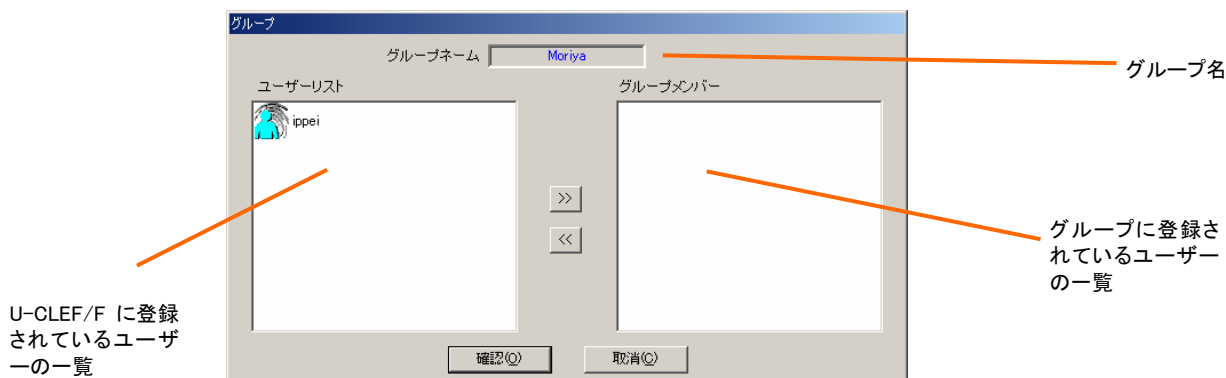
指が濡れている場合もしくは指紋センサーの読み込み面が濡れている場合は、乾いた布等で拭き取って下さい。

センサーの表面は非常に高密度の半導体センサーとなっています。硬い物でこすって傷を付けたり、ぬらさないようにしてください。

センサーの表面は定期的に、やわらかい布などで清掃してください。汚れていると認識率が低下したり、誤認識を起こしたりする場合があります。

グループ機能：

バイオガードセンターに登録されたユーザーは、それぞれ「グループ」に所属させることができます（Windows システムの「ユーザーとパスワード」で定義したグループとは異なります）。そのグループに所属しているメンバーは、グループのユーザーが作成した暗号化ファイルを復号することが可能です。重要なファイルを複数のユーザー間で閲覧したい場合など、グループに登録して利用してください。

たとえば GroupA に UserA,B,C,D の 4 人のユーザーを登録すると、暗号化ファイルの閲覧用に同じキーを保有することになります。グループ管理者はグループ内に新規登録あるいはユーザーを削除する権限があります。たとえバイオガードの上位管理者も該当グループを管理する権限がありません。

グループの編集を行うには、データ設定画面に「グループ」ボタンをクリックします。

すると下の図のようにグループ設定画面が表示します。

左側の「ユーザーリスト」はグループに加入できるユーザーの一覧、右側の「グループメンバー」はメンバーの一覧が表示されます。グループネームは、グループを作成したユーザー名がそのまま自動的に定義されます。

ユーザーをグループに追加するには、ウィンドウ中央部にある「>>」ボタンを押すことによって登録されます。

グループから削除したいユーザーは、右側の「グループメンバー」で選択したあと、「<<」ボタンを押すことによって削除することができます。

使用時間の制限：

管理者は、U-CLEF/F で定義したユーザーに対して、コンピュータの最大利用時間を定義することができます。登録されたアカウントでログオンしたユーザーは、当日に何回ログオンし直しても、通算した使用時間として計算されます。登録した時間を経過してしまうと、翌日以降にならないと、そのユーザーはコンピュータにログオンすることができません。

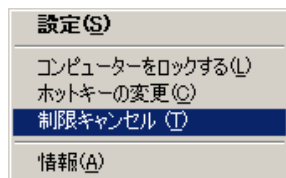
バイオガードセンターをクリックして、設定したいユーザーの「データ設定を開きます。

次に「時間制限」のボタンをクリックして、使用時間を設定します。

“時間制限”のチェックボックスをクリックして、上のプールダウンメニューから使用時間を設定します。（時と分の欄をそのまま空欄にしないで下さい。使用時間を1時間未満の場合、“時”の欄に“00”を選択して下さい。）

時間設定を3分間以上超えると、時間は3分間しかない場合、システムは“コンピュータがシャットダウンしますので、全てのプログラムを閉じて下さい”とのメッセージが現れ、また、画面の右上に赤色の時間ボックスを表示します。

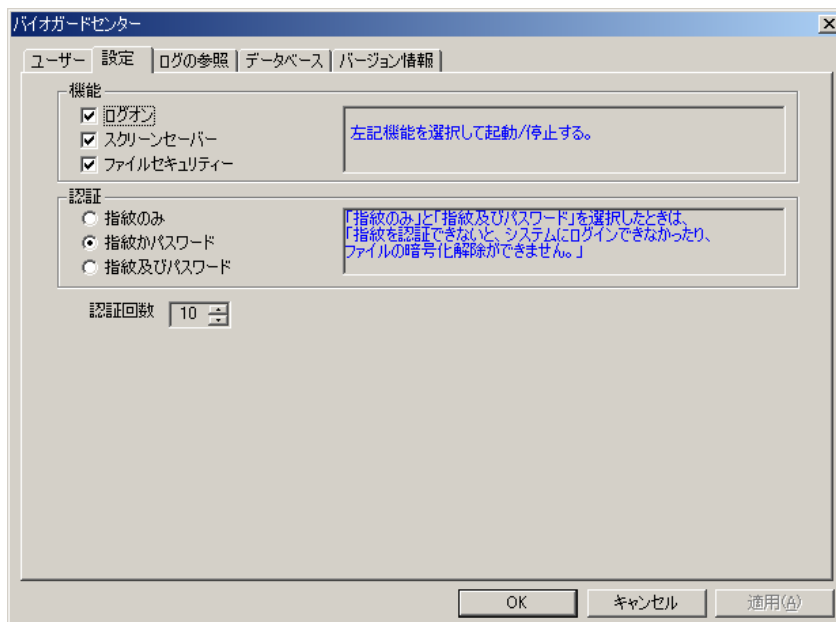
ご注意：

時間の制限は管理者でログオンしたときにしか設定/キャンセルはできません（一般のユーザーはキャンセルできません）。制限のキャンセルには現在登録している状態のみです。ユーザーは再度登録すると、使用時間を引続きカウンダウンします。

注意：

システムのタスクバーに"時間制限"の機能がありますが、それはバイオガードセンターの"時間制限"機能とは異なります。

タスクバーの機能は現在登録しているユーザー（一般ユーザーと管理者）のみ制限します。しかも制限のキャンセルができます。
ユーザーは再度登録すると、前回の時間制限がキャンセルされます。（P.47～48 を参照して下さい）

詳細設定

「設定」では、U-CLEF/F で利用できる機能をオン/オフしたり、認証方式を設定することができます。

➔ 機能

ログオン

Windows システムに指紋登録する機能を起動します。このボックスを選択すれば、次回 Windows システムにログオンする場合、センサーで指紋を認証することが必要です。認証しないと、Windows にログインできません。

もし指紋センサーがコンピュータと接続されていない場合は、「パスワード認証」という画面が表示されますので、登録してあるユーザーの名前とパスワードを入力して登録認証します。正しいアカウントが入力したあと「確認」ボタンをクリックすることによって、Windows システムにログオンすることができます。

指紋センサーがつながっていなかったり不良の場合は、「パスワード認証」の画面が表示され、指紋ではない認証方式でログオンが可能

スクリーンセーバー

バイオガードソフトウェアは Windows に搭載されているスクリーンセーバー機能を拡張して、Windows 通常のスクリーンセーバー機能と同じようにします。さらに従来のパスワード保護機能の代わりに、指紋認証保護の方式になります。 これにより、設定した時間以上経過すると、自動的に PC はロック状態となります。これを解除するには、ログオンしているユーザーが指紋を使って解除しなければなりません。

スクリーンセーバーによるロック機能を利用するには、この画面だけではなく、Windows 側の「画面のプロパティ」での設定も必要です。そのためにはデスクトップ画面にマウスの右ボタンをクリックしてプロパティを選択します。次にスクリーンセーバーラベルをクリックして設定画面を開きます。

画面のプロパティ表示

パスワードによる保護:「パスワードによる保護」のチェックボックスをオンにしたあと、OK ボタンをクリックしてください。

「ファイルセキュリティ」

U-CLEF/F には、コンピュータで作成されたファイルを暗号化して、登録されたユーザーの指紋をキーとして利用する機能が用意されています。この機能を利用することにより、ファイルを暗号化したユーザー以外は、そのファイルを開くことができないようになります。非常に重要なファイルに対してこの機能を利用することにより、何らかのトラブルによってファイルが外部に流失したときにでも、第三者がファイルを開くことはできません。

この機能を利用するには、「ファイルセキュリティ」のチェックボタンをオンにしてください。

➔ 認証

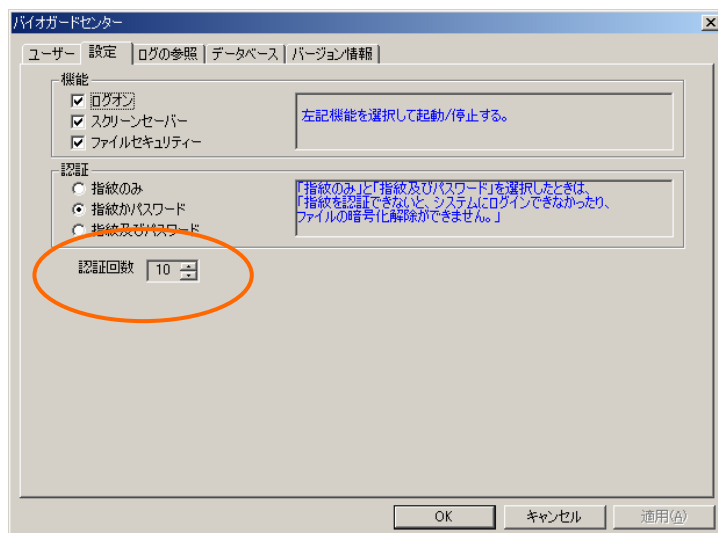
U-CLEF/F では、認証方式として 3 種類用意されている認証方法を選択できすることができます。

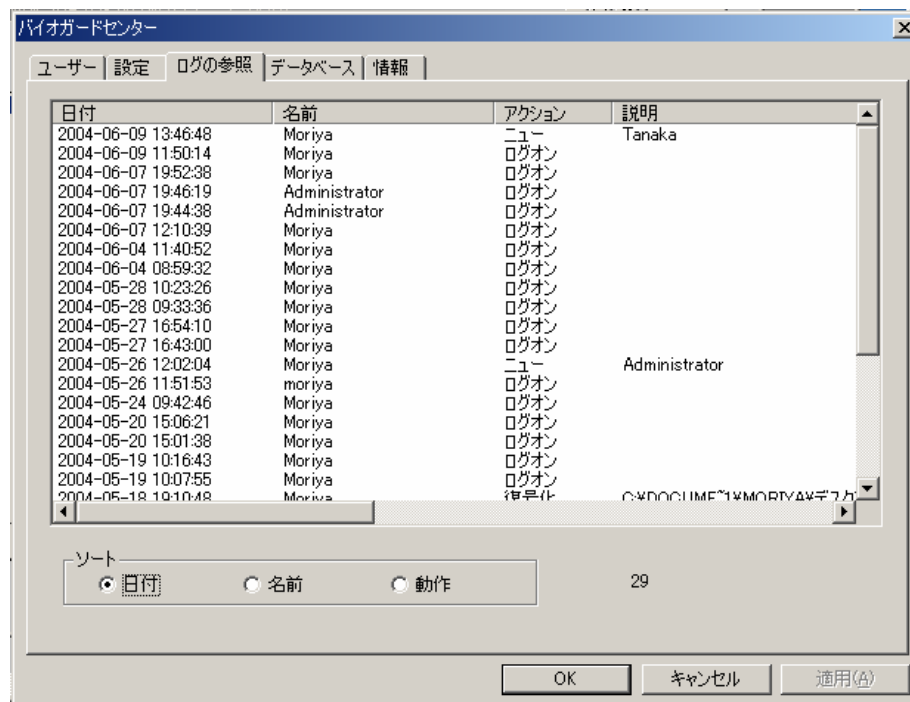
指紋のみ:	センサーから入力された指紋データのみによる認証方式です
指紋かパスワード:	センサーが稼動しているときは指紋データを認証に利用します。センサーが接続されていない場合、もしくはセンサーが故障した場合は、キーボードから入力するパスワードによって認証します(推奨)。
指紋及びパスワード:	センサーから入力された指紋に、さらにパスワードを入力して、両方が適合した場合のみ、認証が正しいと判断します。

"指紋認証"と"指紋及びパスワードの認証"を選択すると、ユーザー自身の指紋しか認証できません。もし指紋センサーが故障あるいは接続されていない場合ログオンすることができなくなるため、通常の利用では「指紋かパスワード」に設定することをお薦めします。

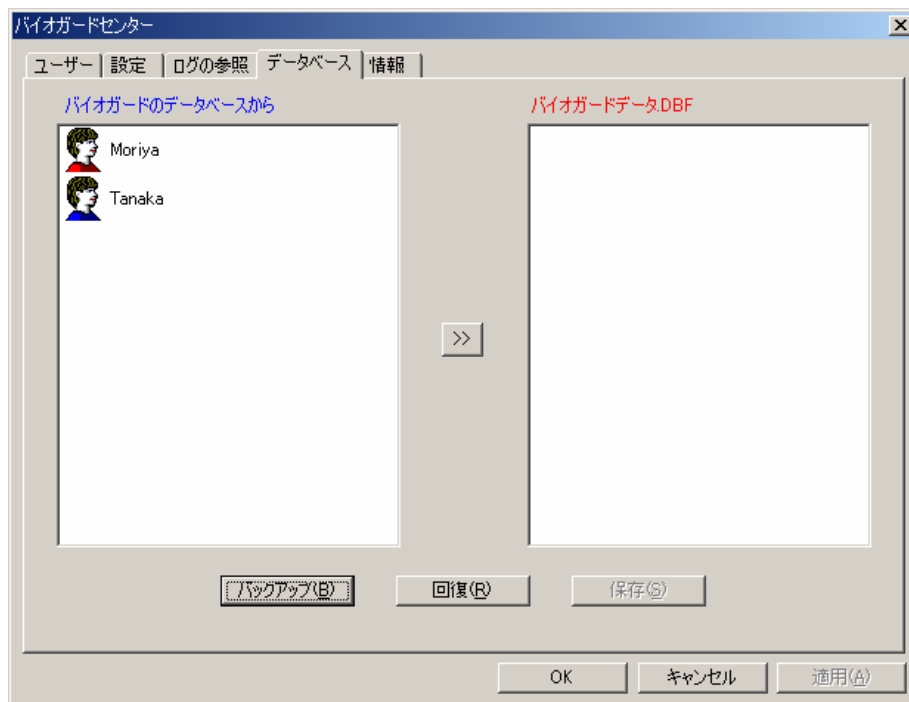
希望する認証方法を選択して、「OK」ボタンをクリックして設定完了です。

➔ 認証回数

「認証回数」を上下の矢印ボタンで調整できます。これは指紋登録の回数です。例えば、"2"を設定すれば、2 回続けて認証に失敗すると、システムが自動的にロックされ、ログオンすることはできなくなります。認証回数は 2～99 回まで設定できます。

ログの参照

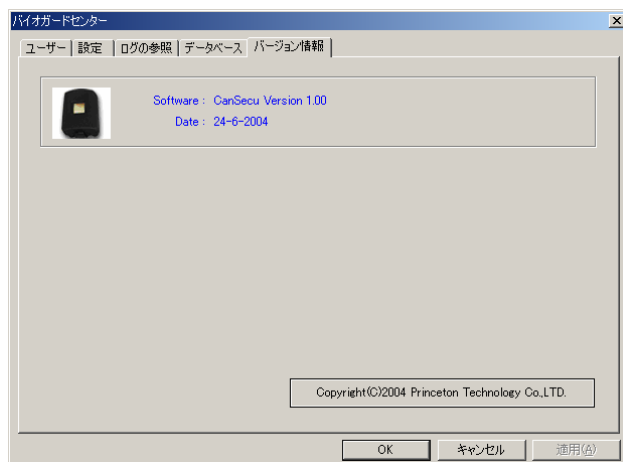
「ログの参照」では、U-CLEF/F が接続されているコンピュータにログオンしたユーザーや、ユーザーの作成情報などを一覧で表示します。

このログ情報は、「日付」「名前」「動作」でソートして表示させることもできます。このログは消去することはできません。

データベースのバックアップ

「データベース」ラベルをクリックして、バイオガードセンターで登録したユーザーのデータをバックアップ することができます。システムの不安定や間違ってユーザーを削除してしまった際に備えてバックアップを取ることをお薦めいたします。

「バックアップ」ボタンをクリックして，ファイルを保存する場所を選択し、ファイル名を入力して保存します。

次に、バックアップしたいユーザーを選択して、→>」ボタンをクリックし、その後、「保存」ボタンをクリックしてバックアップが完了します。データを回復したい場合、「回復」ボタンをクリックしてデータベース(.DBF)を選択して開いて下さい。

情報

「情報」ラベルをクリックして、関連製品及び会社情報が参照できます。

指紋を利用したファイルの暗号化機能

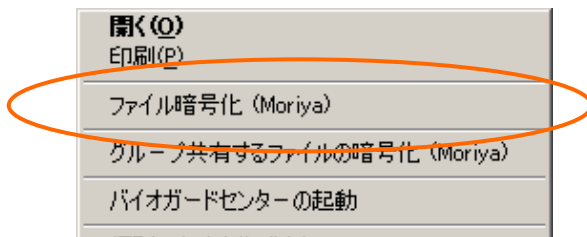
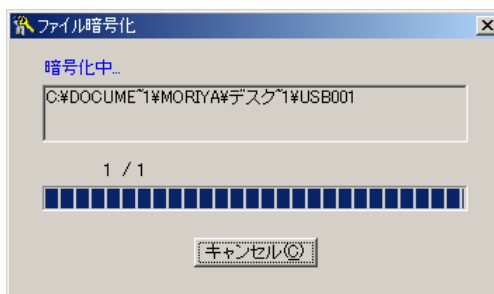
U-CLEF/F には、コンピュータで作成されたファイルを暗号化して、登録されたユーザーの指紋をキーとして利用する機能が用意されています。この機能を利用することにより、ファイルを暗号化したユーザー以外は、そのファイルを開くことができないようになります。非常に重要なファイルに対してこの機能を利用することにより、何らかのトラブルによってファイルが外部に流失したときにでも、第三者がファイルを開くことはできません。
重要なデータは２重も３重も､強固に安全対策を講じることが理想なのです。

U-CLEF/F の暗号化機能

バイオガードソフトウェアは安全性の高いファイルセキュリティ機能があります。暗号化されたファイルは、暗号化したユーザーのみ復号化することができます。そのため、インターネット経由でファイルをやり取りする際にもデータの内容を第三者が判読することが不可能となり、高い安全性を保つことができるようになります。

ご注意：もし暗号化ファイルを作成したユーザーが削除されると、その暗号化されたファイルは復号化することはできません。

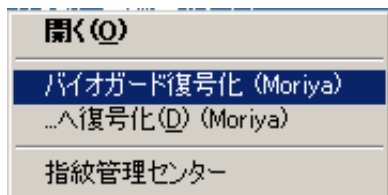
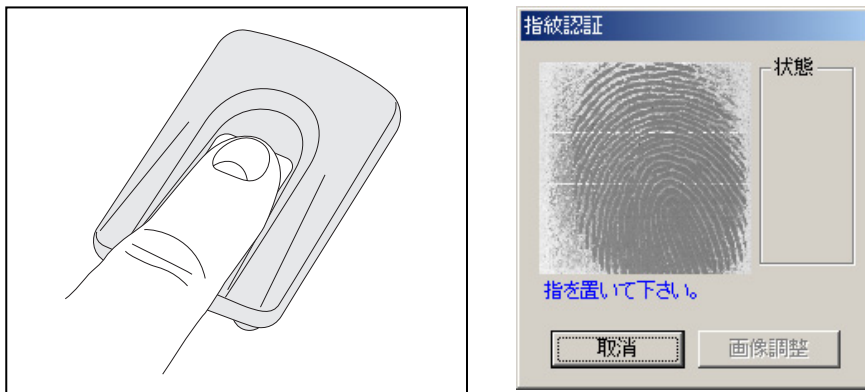
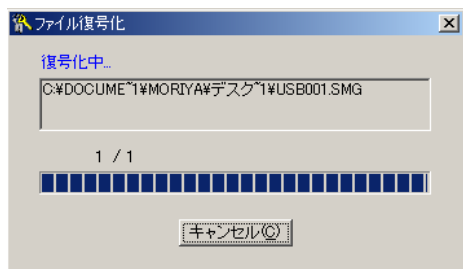
➔ 暗号化ファイルの作成

Windows エクスプローラを開いてファイルやフォルダーを指定するか、ウィンドウにあるファイルを選択してマウスの右ボタンをクリックし、"バイオガード暗号化"との項目を選択することにより、バイオガードセンターはファイルやフォルダーを暗号化します。

この機能は単なるファイルの暗号化だけでなく、複数のファイルやフォルダー、さらにハードディスク全体でも暗号化できます。暗号化機能が使用できるユーザー名が、メニューに表示されます。

暗号化が完了すると、全て暗号化されたファイルが".smz"という拡張子となります。

ご注意：

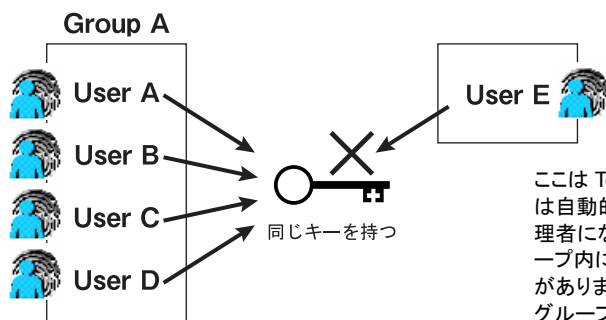
ショートカットアイコンは暗号できませんので、ご注意下さい。 フォルダーに対して暗号化を実行した場合は、フォルダーのなかに含まれているファイル個別に暗号化が行われます。フォルダー全体をひとつの暗号化ファイルとしてまとめることはできませんので、ご注意ください。

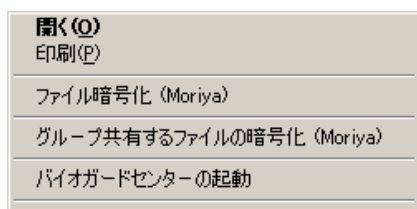
➔ 暗号化ファイルの復元

暗号化されたファイルを復元するには、ファイルをダブルクリックするか、ファイルを選択して右クリックで:表示されるメニューラより、「バイオガード復号化」を選びます。このときポップアップメニューには、ファイルを復号化するための機能がユーザー名が表示されます。

ファイルやフォルダーを復号化する前に指紋認証を必要するため、指紋入力の画面が下記のように表示されます。

ファイルを復号化する権限のあるユーザーの指紋であれば、ファイルの復元化が開始されます。

復号化が完了すると、ファイルタイプやアイコン、そして拡張子も元のものに復元されます。

もし暗号化されたものとは異なる指紋の場合、図のように警告メッセージが表示されますので、正しいユーザーの指紋を認証させるか、指が斜めになっていたり、センサーが汚れていないかを確認してください。

➔ グループ共有するファイル暗号化／復号化機能

選択して、まずアカウントのグループリストが現れて、“>>”あるいは“<<”を通じて、グループメンバーに加入あるいは削除することができます。グループメンバー内のユーザーはグループ管理者が持つ暗号されたファイルを復号する権限を有します。ファイルが移動あるいはコピーされるに関わらず、同じグループ同士は暗号したファイルを復号することができます。

ご注意：バイオガードでのクループ暗号されたファイルは指紋しか復号化できません。パスワードの入力による復元はサポートしていません。

グループでの暗号化したいファイルを選択したあと、マウスボタンの右クリックでメニューを表示させてください。メニューのなかから、「グループ共有するファイルの暗号化」を選択してください。

すると現在ログオンしているユーザーが設定しているグループ情報が表示されます。どのユーザーを登録したいのかが表示されます。

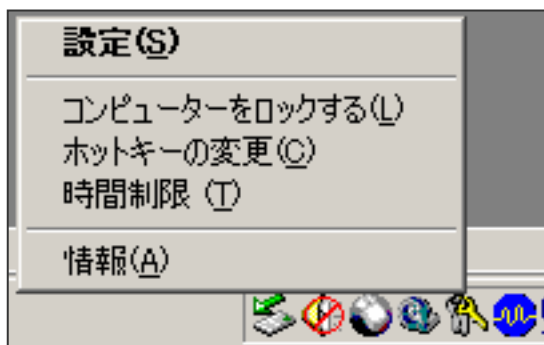
右側に表示されているグループメンバーでよければ「確認」を押して、暗号化を開始してください。

もしグループに追加していないユーザーが左側のユーザーリスト欄にいた場合は、>>ボタンを押して追加したいユーザーをグループに追加してください。

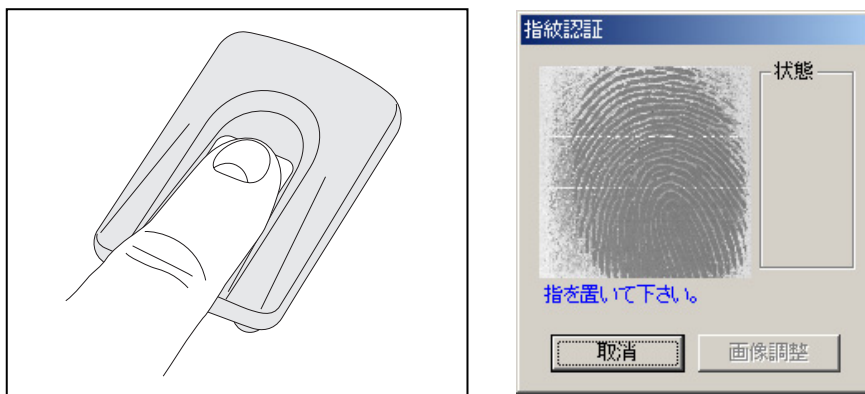
システムトレイに用意された機能

U-CLEF/F では、システムトレイからバイオガードセンターを簡単に呼び出したり、システムを手軽にロックしてセキュリティを高める機能を装備しています。ここでは、システムトレイに用意されている機能と使い方について解説を行います。

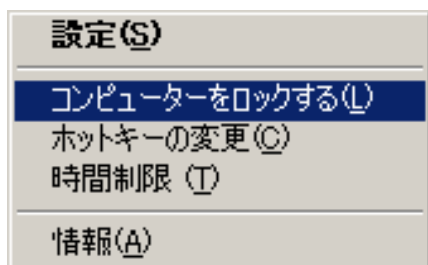
システムトレイの機能

システムトレイ機能は、簡単に機能設定ができるショートカットです。バイオガードをインストール後、システムはタスクバーにキーのアイコンを表示します。 そのアイコンにマウスの右ボタンをクリックすると、下記のようなプログラムメニューが表示されます。

ここで利用できる機能は、下記の 5 つです

設定:	このアイテムをクリックするか、あるいはシステムトレイのキーアイコンをダブルクリックすると、"バイオガードセンター"の画面が開きます。 なお、このときには指紋認証を要求する画面が表示されます。
コンピュータをロックする:	設定されたキーの組み合わせにより、速やかにコンピュータをロック状態にします。
ホットキーの変更:	このアイテムをクリックすると、ホットキーを変更することができます。
使用時間の制限:	指紋アカウントを持つユーザーは"使用時間の制限"機能を設定する権限があります。ユーザーにコンピュータの使用時間を制限して、カウンダウン方式で時間通りにコンピュータをシャットダウンします。操作手順は下記の通りです
情報	バイオガードセンターに関する情報が表示されます

設定

設定を選ぶと、「指紋認証」のウィンドウが表示されます。管理者の指紋を認識されれば、バイオガードセンターの画面が表示されます。

コンピュータをロックする

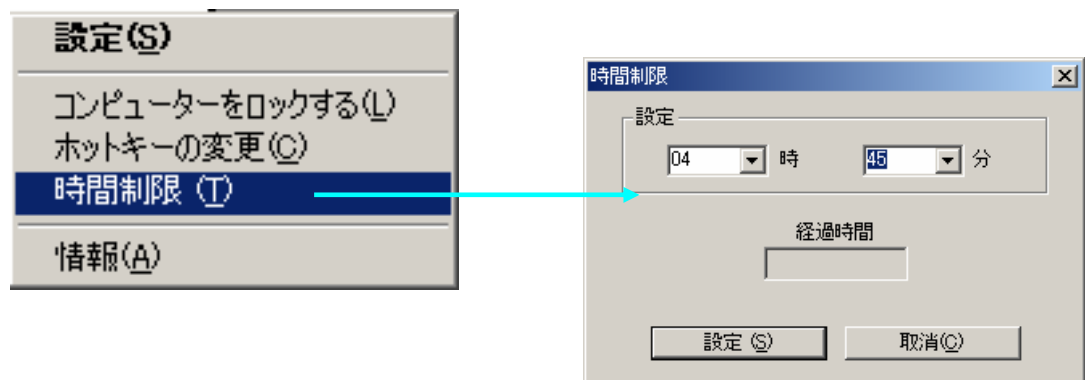
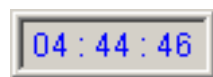
利席する際など、一時的に他人に触らせないように、PC の操作をロックする機能です。

これを選択すると、コンピュータの画面は指紋認証が表示され、それまで利用していたユーザー以外の指紋では、コンピュータを利用することができません。もし異なるユーザーの指紋を認証をさせると、前のユーザーはログオフされてしまいます。

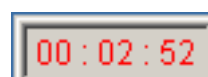
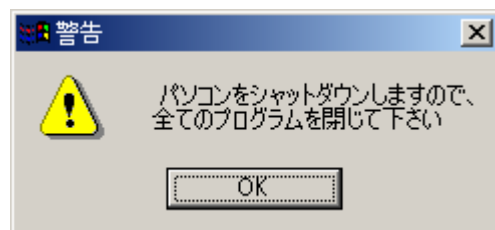
ホットキーの変更

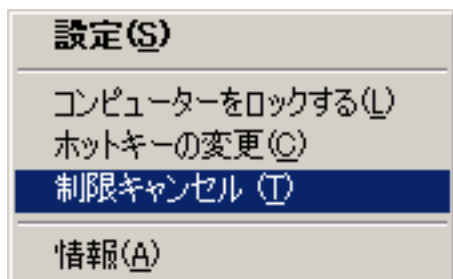
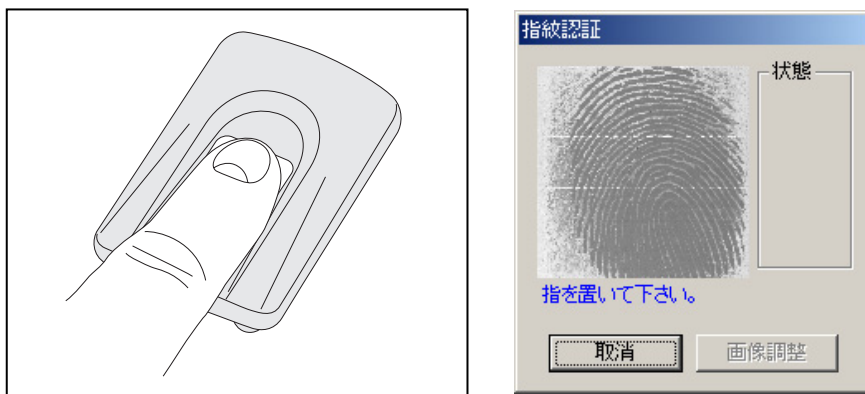
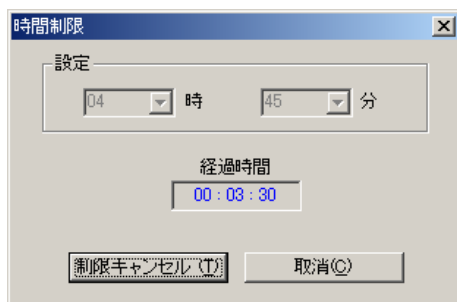
ホットキーを定義しておくことにより、コンピュータをロックするときに、いちいちタスクバーから「コンピュータをロックする」を選ばなくても、ショートカットキーで行うことができるようになります。

時間制限

現在利用しているユーザーに対して、1 日あたり何時間まで利用させることを許可するのかを定義します。

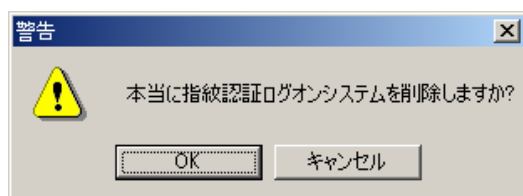
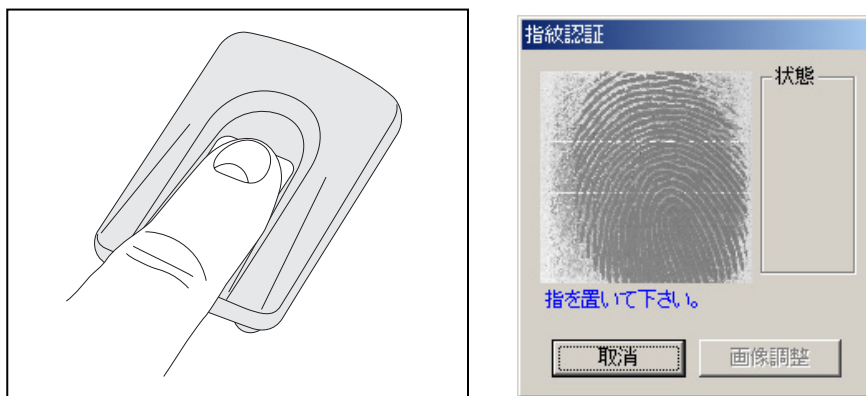
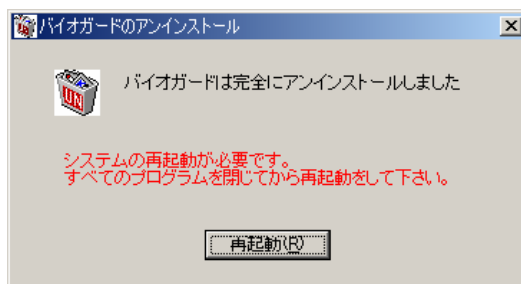
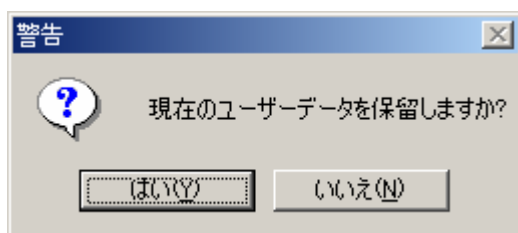
タスクバーから「時間制限」を選択すると、次の画面に“時”と“分”を設定する画面が表示されます。

使用時間をプルダウンから選んで「設定」ボタンをクリックしてから完了です。（注意：“時”の欄は空欄にせず、1 時間未満の場合は“00”をを必ず設定して下さい。）

デスクトップ上に、残り時間を示す時計が表示されます。

使用時間の制限が 3 分を切ると、「コンピュータをシャットダウンしますので、全てのプログラムを閉じて下さい」とのメッセージが表示されます。 あわせてデスクトップ上に表示されている時間表示の文字が赤くなります。そうしたら作業中のデータを保存して、シャットダウンの準備をしてください。

時間制限のキャンセル

時間制限をキャンセルする場合、マウスのカーソルを Windows 画面のタスクバーに移動して、キーのバイオガードアイコンに右ボタンをクリックして、プールダウンメニューに表示される"制限をキャンセル"のアイテムをクリックします。

すると指紋認証画面が表示されますので、現在ログオンしているユーザーの指を指紋センサーに置きます。

「制限を取消」ボタンをクリックして時間制限をキャンセルします。

もし、継続して作業する必要がある場合は、タスクバーのメニューから、「制限キャンセル」を選んでください。これを選ぶと指紋認証の画面が表示され、正しく認識されると、「時間制限」の画面が表示されますので、「制限キャンセル」ボタンを押してください。

U-CLEF/F のアンインストール

バイオガードソフトウェアはアンインストーラーを使用してシステムから完全にソフトウェアを削除することができます。スタート→プログラム→→バイオガード→Un インストール バイオガードを実行します。アンインストールする際に指紋もしくはパスワードの認証確認が必要です。認証確認後、アンインストールプロセスを開始します。

次に、“現在のユーザーデータを保留しますか”とメッセージが現れて、「はい」をクリックして保留するか、「いいえ」をクリックして削除するか選択することができます。最後、システムを再起動してからアンインストールが完了します。

アプリケーションを完全に削除したい場合は、「OK」ボタンを押してください。誤ってアンインストールを選んでしまった場合は、「キャンセル」ボタンを押せば、アンインストール作業は中止させることができます。

もし、現在設定されているユーザー情報などを保管したい場合は「はい（Y）」を、廃棄してもいい場合は「いいえ（N）」ボタンを押してください。

「再起動」ボタンを押して、コンピュータを再起動させてください。

U-CLEF/F の Q&A

ここでは、U-CLEF/F を御使用頂くうえで、疑問に思ったことや、うまく動かなくなったときに役立つ情報をまとめてあります。

Q：システムが指紋センサーを認識できません。マニュアルの指示通りデバイスを抜いて、再度差し込んでも認識しません。なぜでしょうか？

A： 弊社の指紋センサーは USB ケーブルでデバイスと接続しますが、しっかりデバイスと接続しないと認識できない場合があります。 以下のことをお試しください。

・指紋センサーのドライバーのインストールが不完全です。

・ミニ USB コネクターがしっかり指紋センサーと接続しているかどうか、再度確認して下さい。

・ミニ USB コネクターを指紋センサーから抜いて、再度差込んでみてください。カチッと音がしたら、しっかり接続したと確認できます。

・ドライバーを再インストールし直します。

Q：指紋を登録したが、指紋品質の改善、あるいは第二指を登録したい場合、どうすればよいでしょうか？

A：バイオガードソフトウェアを開いて、指紋認証をします。認証確認後、"バイオガードセンター"の画面が開きます。次に「変更」ボタンをクリックすると、"データ設定"の画面が現れます。その中に、"指1"のどれかを選択して、再度指紋を登録して、品質の改善をすることができます。また、"指2"に第二指の指紋登録も可能です。

Q：指紋を登録したが、認証のときにどうしても認識できません、何が問題でしょうか？

A：指紋センサーは様々な状況の指紋(乾、湿、油性)を取込めますが、少し指が濡れていると、よりきれいな指紋画像が得られて認証し易くなります。また、ユーザーはできるだけ"品質A"の指紋を登録するようにお薦めします。品質がよくなると、指紋認識率がもっと高くなります。

"安全レベル"の設定レベルを低くして、より認証し易い状態にしてください。

Q：指紋イメージのデータは、どこに保存されているのか

A：バイオガードは、登録された指紋イメージ全体を保管しているわけではありません。指紋のもつ固有の特徴をデータ化してテンプレートとして保有し、必要な際にセンサーから読み取られた指紋と比較して、正しいものかどうかを判断しています。

登録されたユーザーの指紋全体のイメージは、センサー側にもコンピュータ上にも、一切保有していませんので、ユーザーのプライバシーの保護にもなります。

Q:認証方式を「指紋のみ」にした場合、センサーが破損した場合はログオンする方法はあるのか

A:：「指紋のみ」にした場合は、センサーを利用して指紋によるログオン以外、ログオンする方法はありません。緊急性の高いデータやユーザーの場合は、必ずバ、「指紋かパスワード」に設定してください。この設定であれば、センサーが破損したり紛失した際には、あらかじめ登録してあるユーザー名とパスワードを利用してログオンすることができます。

Q：指紋センサーを接続しているのに、スクリーンセーバー からの回復時に指紋認証画面ではなく、パスワードを要求される。

A：バイオガードセンターのアプリケーションが起動していませんか？ バイオガードセンターを開いている状態でスクリーンセーバーが起動した場合、指紋認証画面ではなく、ユーザー名/パスワードを尋ねる画面が表示されます。

Q：「FRR」、「FAR」とは何ですか？

A：
・FRR：本人拒否率
 照合時、誤って本人を他人と判定して照合が失敗する比率です。
・FAR：他人受容率
 照合時、誤って他人を本人と判定して照合してしまう比率です。

Q：指が荒れていても登録／照合はできますか？

A： 皮膚が極端に荒れている指、極端に乾いたり湿ったりしている指は登録しにくい場合があります。
その場合は、別の指を使って登録していただきます。

Q：指に傷があっても登録／照合はできますか？

A：多少の傷があっても、特徴点の抽出ができれば照合できます。
傷がひどい場合は、あらかじめ登録してある別の指を使用していただきます。

製品保証に関して

・万一、製品のご購入から 1 年以内に製品が故障した場合は、弊社による故障判断完了後、無償にて修理/製品交換対応させていただきます。修理にて交換された本体および部品に関しての所有権は弊社に帰属するものと致します。

・保証の対象となる部分は製品のハードウェア部分のみで、添付品や消耗品は保証対象より除外とさせていただきます。

・本製品の故障また使用によって生じた損害は、直接的・間接的問わず、弊社は一切の責任を負いかねますので、予めご了承ください。

・当社は商品どうしの互換性問題やある特定用途での動作不良や欠陥などの不正確な問題に関する正確性や完全性については、黙示的にも明示的にもいかなる保証も行なっておりません。また販売した商品に関連して発生した下記のような障害および損失についても、当社は一切の責任を負わないものといたします。

・一度ご購入いただいた商品は、商品自体が不良ではない限り、返品または交換はできません。各機器には対応機種があり、ご購入時にご案内していますのでよくご確認下さい。対応機種間違いによる返品はできませんので予めご了承下さい。

This warranty is valid only in Japan

保証期間　御購入日より 1 年間

●お買い上げになりました機器が、取扱説明書等に従った正常な使用状態で万一故障した場合には、本保証規定に従い無料にて故障の修理をいたします。

●修理の際には製品と本保証書をご提示または添付の上、ご依頼ください。

●保証期間内でも次の場合には有償修理となる場合がございます。

1) ユーザー登録をされていない場合。

2) 本保証書をご提示されない場合、または記入もれ、改ざん等が認められた場合。

3) ご使用の誤り、または不等な修理、調整、改造、誤接続による故障及び損傷が認められた場合。

4) 接続している他の機器に起因して生じた故障及び損傷。

5) お買い上げ後の輸送や移動、落下等不当なお取り扱いにより生じた故障及び損傷。

6) 火災、天災、公害、塩害、異常電圧や指定外の電圧使用等による故障及び損傷。

●本保証書は、日本国内においてのみ有効です。This warranty is valid only in Japan

●免責事項、製品保証に関しての記載も併せてご覧ください。

免責事項

■保証期間内であっても、次の場合は保証対象外となります。

・保証書のご提示がない場合、または記入漏れ、改ざん等が認められた場合。

・設備、環境の不備等、使用方法および、注意事項に反するお取り扱いによって生じた故障・損傷。

・輸送・落下・衝撃など、お取り扱いが不適切なために生じた故障・損傷。

・お客様の責に帰すべき事由により生じた機能に影響のない外観上の損傷。

・火災、地震、水害、塩害、落雷、その他天地異変、異常電圧などにより生じた故障・損傷。

・接続しているほかの機器、その他外部要因に起因して生じた故障・損傷。

・お客様が独自にインストールされたソフトウェアに起因して生じた故障・損傷。

・お客様の故意または重過失により生じた故障・損傷。

・ユーザーズガイド記載の動作条件ならびに機器設置環境を満足していない場合。

・弊社もしくは弊社指定の保守会社以外で本製品の部品交換・修理・調整・改造を施した場合。

■お買い上げ製品の故障もしくは動作不具合により、その製品を使用したことにより生じた直接、間接の損害、HDD 等記憶媒体のデータに関する損害、逸失利益、ダウンタイム（機能停止期間）、顧客からの信用、設備および財産への損害、交換、お客様および関係する第三者の製品を含むシステムのデータ、プログラム、またはそれらを修復する際に生じる費用（人件費、交通費、復旧費）等、一切の保証は致しかねます。 またそれらは限定保証の明記がされていない場合であっても（契約、不法行為等法理論の如何を問わず）責任を負いかねます。

■製品を運用した結果の他への影響につきましては一切の責任を負いかねますので予めご了承下さい

■指紋を認証できなかったことによって発生する動作障害、データの損失、あるいは他の偶発的または必然的な損害（経済的、

時間的、業務的、精神的等）に対しては、弊社では一切の責任を負いかねます

■購入された当社製品の故障、または当社が提供した保証サービスによりお客様が被った損害（経済的、時間的、業務的、精神的等）のうち、直接・間接的に発生する可能性のあるいかなる逸失利益、損害につきましては、当社に故意または重大なる過失がある場合を除き、弊社では一切責任を負いかねますのでご了承ください。また、弊社が責任を負う場合でも、重大な人身損害の場合を除き、お客様が購入された弊社製品などの価格を超えて責任を負うものではありません。

製品保証規定

製品修理に関して

* 保証期間内の修理は、弊社テクニカルサポートまでご連絡いただいた後、故障品を弊社まで送付していただきます。修理完了品または代替品をご指定の場所にご送付させて頂きます。
* 動作確認作業中及び修理中の代替品・商品貸し出し等はいかなる場合においても一切行っておりません。
* お客様に商品が到着した日から 1 週間以内に、お客様より当社に対して初期不良の申請があった場合で、なおかつ弊社側の認定がなされた場合にのみ初期不良品として、正常品もしくは新品との交換をさせていただきます。その際はご購入時の梱包、箱、保証書などの付属品等が全て揃っていることが条件となります。
* 修理品に関しては「製品保証書」を必ず同梱し、下記「お問い合わせについて」に記入された住所までご送付ください。
* 製造中止等の理由により交換商品が入手不可能な場合には同等品との交換となります。
* お客様の設定、接続等のミスであった場合、また製品の不良とは認められない場合は、技術料およびチェック料を頂く場合がございますので予めご了承下さい。
* お客様の御都合により、有料修理の撤回・キャンセルを行われた場合は技術作業料及び運送料を請求させて頂く場合がございますので予めご了承下さい。
* サポートスタッフの指示なく、お客様の判断により製品をご送付頂いた場合で、症状の再現性が見られない場合、及び製品仕様の範囲内と判断された場合、技術手数料を請求させて頂く場合がございますので予めご了承下さい。

お問い合せについて

カスタマーサポート・保証に関するお問い合わせ先

受付期間　月曜～金曜日　午前 9 時～午前 12 時　午後 1 時～午後 5 時半

（土曜、年末年始、祝日、祭日、国民の休日を除く）

〒101-0032 東京都千代田区岩本町 3-9-5 K.A.I.ビル 3F

プリンストンテクノロジー株式会社　テクニカルサポート課

フリーダイヤル：0120-262-686／FAX：03-3863-7451

サポート専用 Web ページ：http://www.princeton.co.jp/support/top.html

故障、不具合などが発生した場合は、下記の項目をお伝えいただけますよう、お願い申し上げます。